AMENDMENT TO THE CLAIMS

The following listing of claims replaces all prior versions and listings:

1. (Previously Presented) A computer system providing Internet protocol security without secure domain name resolution, the system comprising:

a local domain name service (DNS) server that is communicatively coupled to a processor and that includes a secure Internet security protocol (IPSEC) cache, wherein the secure IPSEC cache comprises a plurality of cache entries, wherein each cache entry comprises a domain name and information that uniquely associates the cache entry with a particular application process or execution time, wherein the secure IPSEC cache is readable only by an Internet protocol (IP) processing layer of an operating system that controls execution of an application program by the processor;

a security policy data store that is communicatively coupled to the IP processing layer;

a computer-readable medium accessible to the processor and comprising one or more sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving a message generated as a result of execution of the application program and that contains a domain name to be resolved by the local DNS server;

storing, in a first of the cache entries, the domain name contained in the message and identifying information that uniquely associates the first cache entry with a particular application process or execution time;

receiving a data packet from the application;

in response to receiving the data packet from the application, locating an entry in the secure IPSEC cache,

based on the identifying information in the located cache entry, verifying that the domain name in the located entry matches the domain name in the message;

querying the security policy data store for an IPSEC policy matching the domain name in the located entry, wherein the IP processing layer verifies that the policy matches the domain name contained in the message;

in response to obtaining an IPSEC policy, applying the IPSEC policy to the data packet; and

purging the matching entry from the cache.

2. (Previously Presented) A computer system as recited in Claim 1, wherein each cache entry further comprises one or more IP addresses that correspond to the domain name for the entry.

3. (Previously Presented) A computer system as recited in Claim 2, wherein the step of verifying that the domain name in the located entry matches the domain name contained in the message further comprises the step of searching the secure IPSEC cache for an entry that matches a process identifier of the application program.

4. (Previously Presented) A computer system as recited in Claim 2, wherein the information, for each cache entry, that uniquely associates the cache entry with a particular application process or execution time comprises a process identifier value and a transaction identifier value.

5. (Previously Presented) A computer system as recited in Claim 4, wherein the step of verifying that the domain name in the located entry matches the domain name contained in the message further comprises the step of searching the secure IPSEC cache for an entry that matches a process and transaction associated with the application program.

6. (Previously Presented) A computer system as recited in Claim 1, further comprising the step of querying the security policy database for an IPSEC policy based on an IP address that is resolved from the domain name received from the application program only when a matching cache entry is not found by searching the cache based on the domain name.

7. (Currently Amended) A computer system as recited in Claim 1, further comprising the steps of:

wherein the message is a request to resolve the domain name into network addresses;

resolving the domain name using the local DNS server, resulting in generating one or more network addresses corresponding to the domain name;

determining the identifier information that uniquely associates the request with a particular application process or execution time; and

storing the [[the]] network addresses in the first cache entry of the secure IPSEC cache.

8. (Previously Presented) A method for providing Internet protocol security without secure domain name resolution, the method comprising the computer-implemented steps of:

receiving a message generated as a result of execution of an application program and that contains a domain name to be resolved by the local DNS server;

storing, in a first cache entry of a secure Internet security protocol (IPSEC) cache, the domain name contained in the message and identifying information that uniquely associates the first cache entry with a particular application process or execution time, wherein the secure IPSEC cache is communicatively coupled to a local domain name service (DNS) server, and wherein the secure IPSEC cache is readable only by an Internet protocol (IP) processing layer of an operating system that controls execution of the application program, and wherein each cache entry comprises information that uniquely associates the cache entry with a particular application process or execution time;

receiving a data packet from the application;

in response to receiving the data packet from the application, locating an entry in the secure IPSEC cache;

based on the identifying information in the located cache entry, verifying that the domain name in the located entry matches the domain name in the message;

in response to obtaining an IPSEC policy, querying a security policy data store that is communicatively coupled to the IP processing layer for an IPSEC policy matching the domain name in the located entry, wherein the IP processing layer verifies that the policy matches the domain name contained in the message;

applying the IPSEC policy to the data packet; and

purging the matching entry from the cache.

9. (Previously Presented) A method as recited in Claim 8, wherein each cache entry further comprises one or more IP addresses that correspond to the domain name for the entry.

10. (Previously Presented) A method as recited in Claim 9, wherein the step of verifying that the domain name in the located entry matches the domain name contained in the message further comprises the step of searching the secure IPSEC cache for an entry that matches a process identifier of the application program.

11. (Previously Presented) A method as recited in Claim 9, wherein the information, for each cache entry, that uniquely associates the cache entry with a particular application process or execution time comprises a process identifier value and a transaction identifier value.

12. (Previously Presented) A method as recited in Claim 11, wherein the step of verifying that the domain name in the located entry matches the domain name contained in the message further comprises the step of searching the secure IPSEC cache for an entry that matches a process and transaction associated with the application program.

13. (Previously Presented) A method as recited in Claim 8, further comprising the step of querying the security policy database for an IPSEC policy based on an IP address that is resolved from the domain name received from the application program only when a matching cache entry is not found by searching the cache based on the domain name.

14. (Previously Presented) A method as recited in Claim 8, further comprising the steps of:

wherein the message is a request to resolve the domain name into network addresses;

resolving the domain name using the local DNS server, resulting in generating one or more network addresses corresponding to the DNS name;

determining the identifier information that uniquely associates the request with a particular application process or execution time; and

storing the network addresses in the first cache entry of the secure IPSEC cache.

15. (Previously Presented) A computer-readable medium carrying one or more sequences of instructions for providing Internet protocol security without secure domain name resolution, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving a message generated as a result of execution of an application program and that contains a domain name to be resolved by the local DNS server;

storing, in a first cache entry of a secure Internet security protocol (IPSEC) cache, the domain name contained in the message and identifying information that uniquely associates the first cache entry with a particular application process or execution time, wherein the secure IPSEC cache is communicatively coupled to a local domain name service (DNS) server, and wherein the secure IPSEC cache is readable only by an Internet protocol (IP) processing layer of an operating system that controls execution of the application program, and wherein each cache entry comprises information that uniquely associates the cache entry with a particular application process or execution time;

receiving a data packet from the application;

in response to receiving the data packet from the application, locating an entry in the secure IPSEC cache;

based on the identifying information in the located cache entry, verifying that the domain name in the located entry matches the domain name in the message;

in response to obtaining an IPSEC policy, querying a security policy data store that is communicatively coupled to the IP processing layer for an IPSEC policy matching the domain name in the located entry, wherein the IP processing layer verifies that the policy matches the domain name contained in the message;

applying the IPSEC policy to the data packet; and

purging the matching entry from the cache.

16-21. (Canceled)

22. (Previously Presented) An apparatus for providing Internet protocol security without secure domain name resolution, comprising:

means for receiving a message generated as a result of execution of an application program and that contains a domain name to be resolved by the local DNS server;

means for storing, in a first cache entry of a secure Internet security protocol (IPSEC) cache, the domain name contained in the message and identifying information that uniquely associates the first cache entry with a particular application process or execution time, wherein the secure IPSEC cache is communicatively coupled to a local domain name service (DNS) server, and wherein the secure IPSEC cache is readable only by an Internet protocol (IP) processing layer of an operating system that controls execution of the application program, and wherein each cache entry comprises information that uniquely associates the cache entry with a particular application process or execution time;

means for receiving a data packet from the application;

in response to receiving the data packet from the application, means for locating an entry in the secure IPSEC cache;

based on the identifying information in the located cache entry, means for verifying that the domain name in the located entry matches the domain name in the message;

means for querying a security policy data store that is communicatively coupled to the IP processing layer for an IPSEC policy matching the domain name in the located entry, wherein the IP processing layer verifies that the policy matches the domain name contained in the message;

means for applying the IPSEC policy to the data packet; and

means for purging the matching entry from the cache.

23. (Previously Presented) An apparatus for providing Internet protocol security, without secure domain name resolution, for messages that are carried by a packet-switched data network, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving a message generated as a result of execution of an application program and that contains a domain name to be resolved by the local DNS server;

storing, in a first cache entry of a secure Internet security protocol (IPSEC) cache, the domain name contained in the message and identifying information that uniquely associates the first cache entry with a particular application process or execution time, wherein the secure IPSEC cache is communicatively coupled to a local domain name service (DNS) server, and wherein the secure IPSEC cache is readable only by an Internet protocol (IP) processing layer of

an operating system that controls execution of the application program, and

wherein each cache entry comprises information that uniquely associates the cache entry with a particular application process or execution time;

receiving a data packet from the application;

in response to receiving the data packet from the application, locating an entry in the secure IPSEC cache;

based on the identifying information in the located cache entry, verifying that the domain name in the located entry matches the domain name in the message;

in response to obtaining an IPSEC policy, querying a security policy data store that is communicatively coupled to the IP processing layer for an IPSEC policy matching the domain name in the located entry, wherein the IP processing layer verifies that the policy matches the domain name contained in the message;

applying the IPSEC policy to the data packet; and

purging the matching entry from the cache.

24. (Previously Presented) An apparatus as recited in Claim 22, wherein each cache entry further comprises one or more IP addresses that correspond to the domain name for the entry.

25. (Previously Presented) A apparatus as recited in Claim 24, wherein the means for verifying that the domain name in the located entry matches the domain name

contained in the message further comprises means for searching the secure IPSEC cache for an entry that matches a process identifier of the application program.

26. (Previously Presented) A apparatus as recited in Claim 25, wherein the information, for each cache entry, that uniquely associates the cache entry with a particular application process or execution time comprises a process identifier value and a transaction identifier value.

27. (Previously Presented) A apparatus as recited in Claim 26, wherein the means for verifying that the domain name in the located entry matches the domain name contained in the message further comprises means for searching the secure IPSEC cache for an entry that matches a process and transaction associated with the application program.

28. (Previously Presented) A apparatus as recited in Claim 22, further comprising means for querying the security policy database for an IPSEC policy based on an IP address that is resolved from the domain name received from the application program only when a matching cache entry is not found by searching the cache based on the domain name.

29. (Currently Amended) An apparatus as recited in Claim 22, wherein the message is a request to resolve the domain name into network addresses; and further comprising:

means for resolving the domain name the local DNS server, resulting in generating one or more network addresses corresponding to the domain name;

means for determining identifier information that uniquely associates the request with a particular application process or execution time; and

means for storing the network addresses as an entry in the secure IPSEC cache.